EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	(("6,539,380") or ("6,115,819")).PN.	US-PGPUB; USPAT	OR	OFF	2007/07/24 23:00
S2	1882	(713/193).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/08/31 21:08
S3	225	S2 and (protected near4 (address memory))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/24 23:01
S4	2	("5787367" | "5844986").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/24 23:03
S5	6	("6757832").URPN.	USPAT	OR	ON	2007/07/24 23:03
S6	1	("20040255145").PN.	US-PGPUB; USPAT	OR	OFF	2007/08/31 20:10
S7	1943	(713/193).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/09/01 12:38
S8	96	S7 and (key adj store)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/31 21:13
S9	0	S7 and single adj use near4 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/31 21:13
S10	190	S7 and (remov$3 delet$3 destroy$3) near3 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/31 23:33
S11	23	S7 and (remov$3 delet$3 destroy$3) near3 key and key adj store	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:16

EAST Search History

S12	18	("4135240" | "4506329" | "4590552" | "4884211" | "4954982" | "5146565" | "5187790" | "5280527" | "5500517" | "5566327" | "5581700" | "5719950" | "5724578" | "5805719" | "5936221" | "6040622" | "6147860" | "6240493").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/08/31 22:29
S13	1	("6539380").URPN.	USPAT	OR	ON	2007/08/31 22:31
S14	6	("6115819").URPN.	USPAT	OR	ON	2007/08/31 22:32
S15	1	("7194092").URPN.	USPAT	OR	ON	2007/08/31 22:32
S16	109	("20020007452" | "20020069365" | "20020107803" | "20020120936" | "20020152173" | "4827508" | "4969189" | "4977594" | "5007082" | "5023907" | "5050213" | "5140634" | "5276311" | "5335334" | "5349643" | "5410598" | "5473690" | "5473692" | "5491827" | "5544246" | "5557518" | "5557765" | "5623637" | "5654746" | "5664016" | "5671280" | "5721781" | "5745886" | "5757919" | "5796824" | "5802592" | "5812662" | "5812980" | "5841869" | "5860099" | "5872847" | "5892900" | "5892902" | "5892904" | "5910987" | "5915019" | "5917912" | "5919257" | "5920861" | "5933498" | "5940504" | "5943422" | "5944821" | "5949876" | "5953502" | "5958050" | "5963980" | "5974546" | "5982891" | "5991399" | "5991876" | "6006332" | "6009274" | "6009401" | "6026166" | "6032257" | "6038551" | "6073124" | "6092189" | "6105137" | "6112181" | "6118873" | "6138119" | "6148083" | "6148387" | "6148402" | "6157721" | "6175917" | "6185678" | "6185683" | "6189100" | "6192473" | "6212636" | "6223284" | "6229894" | "6230285" | "6237786" | "6240185" | "6253193" | "6263431" | "6272629" | "6292569" | "6327652" | "6327660" | "6330588" | "6338139" | "6341373" | "6363486" | "6363488" | "6367012" | "6381741" | "6389402" | "6389537" | "6427140" | "6449367" | "6477252" | "6477648" | "6480961" | "6560706" | "6609199" | "6640304" | "6735696" | "6820063" | "7079649").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/08/31 22:37
S17	336	(713/190).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/08/31 23:58

EAST Search History

S18	23	S17 and (remov$3 delet$3 destroy$3) near3 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/31 23:33
S19	1	("20020174352").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 00:07
S20	1	("5751949").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 00:08
S21	43	key adj store same (file near2 name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 00:08
S22	4	("20020071556" | "5931947" | "6249866" | "6678700").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/09/01 02:14
S23	14	protected near3 memory near3 (address$2 location) and key adj store	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:22
S24	2	protected near3 memory same key adj store same memory adj access	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:23
S25	2	protected near3 memory same key adj store and memory adj access	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:23
S26	4375	((secure$1 protected)near3 memory).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:24
S27	441	((secure$1 protected) near3 memory and key).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:25

EAST Search History

S28	386	((protect$3) near3 memory and key).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 02:26
S29	70	((protect$3) near3 memory and key).ab.	US-PGPUB; USPAT	OR	ON	2007/09/01 02:26
S30	34	("4038645").URPN.	USPAT	OR	ON	2007/09/01 02:27
S31	1	("6578122").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 12:38
S32	1	("6539380").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 12:38
S33	105	(713/192).CCLS.	USPAT	OR	OFF	2007/09/01 12:39
S34	1074	(711/163).CCLS.	USPAT	OR	OFF	2007/09/01 12:40
S35	1	S34 and (infiniband).ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 12:40
S36	159	infiniband.ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/01 12:50
S37	1	("20020124148").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 22:05
S38	1	("5751949").PN.	US-PGPUB; USPAT	OR	OFF	2007/09/01 22:06
S39	5	("5574849" | "5684993" | "5915088" | "6163834" | "6349380").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/09/01 22:12
S40	5	("5574849" | "5684993" | "5915088" | "6163834" | "6349380").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/09/01 22:12
S41	5	("5574849" | "5684993" | "5915088" | "6163834" | "6349380").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/09/01 22:12
S42	6	("6578122").URPN.	USPAT	OR	ON	2007/09/01 22:13
S43	10	("20020078271" | "20020124117" | "20020124148" | "20020178339" | "20020184392" | "20030046505" | "6578122" | "6601148" | "6658521" | "6691217").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/09/01 22:14

Terms used: **storage protection access encryption key** Found **1,214** of **209,709**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems
Vishal Kher, Yongdae Kim
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

2 Improved proxy re-encryption schemes with applications to secure distributed storage
Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger
February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1
Publisher: ACM Press
Full text available: pdf(331.59 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

3 Access management for distributed systems: Peer-to-peer access control architecture using trusted computing technology
Ravi Sandhu, Xinwen Zhang

June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies SACMAT '05**
Publisher: ACM Press

Full text available: pdf(215.48 KB) Additional Information: full citation, abstract, references, citings, index terms, review

It has been recognized for some time that software alone does not provide an adequate foundation for building a high-assurance trusted platform. The emergence of industry-standard trusted computing technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for security in peer-to-peer environments. In this paper we propose a trusted computing architecture to enforce ac ...

Keywords: access control, policy enforcement, security architecture, trusted computing

4 Cryptographic storage security: Secure capabilities for a petabyte-scale object-based distributed file system
Christopher Olson, Ethan L. Miller
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(199.37 KB) Additional Information: full citation, abstract, references, index terms

Recently, the Network-Attached Secure Disk (NASD) model has become a more widely used technique for constructing large-scale storage systems. However, the security system proposed for NASD assumes that each client will contact the server to get a capability to access one object on a server. While this approach works well in smaller-scale systems in which each file is composed of a few objects, it fails for large-scale systems in which thousands of clients make accesses to a single file composed ...

Keywords: capabilities, object-based storage, scalability

5 Architecture for Protecting Critical Secrets in Microprocessors
Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang
May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd annual international symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2
Publisher: IEEE Computer Society, ACM Press
Full text available: pdf(143.62 KB) Additional Information: full citation, abstract, cited by, index terms

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem ¿ often assumed but not solved ¿ underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

6 Cryptographic storage security: Key management for multi-user encrypted databases
Ernesto Damiani, S. De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(408.91 KB) Additional Information: full citation, abstract, references, index terms

Database outsourcing is becoming increasingly popular introducing a new paradigm, called *database-as-a-service* (DAS), where an organization's database is stored at an external service provider. In such a scenario, access control is a very important issue, especially if the data owner wishes to publish her data for external use.In this paper, we first present our approach for the implementation of access control through selective encryption. The focus of the paper is then the presentation ...

Keywords: encrypted/indexing databases, hierarchical key derivation schema, selective access

7 Data protection: Searchable symmetric encryption: improved definitions and efficient constructions

Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

Publisher: ACM Press

Full text available: pdf(682.40 KB) Additional Information: full citation, abstract, references, index terms

Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties:

1. Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per r ...

Keywords: multi-user, searchable encryption, searchable symmetric encryption, security definitions

8 General storage protection techniques: Ensuring data integrity in storage: techniques and applications

Gopalan Sivathanu, Charles P. Wright, Erez Zadok

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available: pdf(217.83 KB) Additional Information: full citation, abstract, references, index terms

Data integrity is a fundamental aspect of storage security and reliability. With the advent of network storage and new technology trends that result in new failure modes for storage, interesting challenges arise in ensuring data integrity. In this paper, we discuss the causes of integrity violations in storage and present a survey of integrity assurance techniques that exist today. We describe several interesting applications of storage integrity checking, apart from security, and discuss the im ...

Keywords: file systems, intrusion detection, storage integrity

9 A key distribution method for object-based protection

Warwick Ford, Michael J. Wiener

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security CCS '94**

Publisher: ACM Press

Full text available: pdf(501.57 KB) Additional Information: full citation, abstract, references, index terms

In any scheme for protecting the confidentiality of data, selecting a key and encrypting

the data is the easy part. The difficult part is controlling access to decryption keys. This becomes particularly significant with object-based protection, that is protection of an object, such as a file or a message, regardless of where the object is currently being stored or transferred within a distributed environment. An example of object-based protection is traditional electronic m ...

10 Short papers -- storage survivability: Toward securing untrusted storage without public-key operations

Dalit Naor, Amir Shenhav, Avishai Wool

November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**

Publisher: ACM Press

Full text available: pdf(344.77 KB) Additional Information: full citation, abstract, references, index terms

Adding security capabilities to shared, remote and untrusted storage file systems leads to performance degradation that limits their use. Public-key cryptographic primitives, widely used in such file systems, are known to have worse performance than their symmetric key counterparts. In this paper we examine design alternatives that avoid public-key cryptography operations to achieve better performance. We present the trade-offs and limitations that are introduced by these substitutions.

Keywords: network attached storage, secure file systems

11 Intrusion detection and modeling: Augmenting storage with an intrusion response primitive to ensure the security of critical data

Ashish Gehani, Surendar Chandra, Gershon Kedem

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(326.59 KB) Additional Information: full citation, abstract, references, index terms

Hosts connected to the Internet continue to suffer attacks with high frequency. The use of an intrusion detector allows potential threats to be flagged. When an alarm is raised, preventive action can be taken. A primary goal of such action is to assure the security of the data stored in the system. If this operation is effected manually, the delay between the alarm and the response may be enough for an intruder to cause significant damage.The alternative proposed in this paper is to provide a re ...

12 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

13 Decentralized storage systems: Farsite: federated, available, and reliable storage for an incompletely trusted environment

Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger P. Wattenhofer
December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Publisher: ACM Press
Full text available: pdf(1.87 MB) Additional Information: full citation, abstract, references, cited by, index terms

Farsite is a secure, scalable file system that logically functions as a centralized file server but is physically distributed among a set of untrusted computers. Farsite provides file availability and reliability through randomized replicated storage; it ensures the secrecy of file contents with cryptographic techniques; it maintains the integrity of file and directory data with a Byzantine-fault-tolerant protocol; it is designed to be scalable by using a distributed hint mechanism and delegatio ...

14 Scaling security: Design, implementation and evaluation of security in iSCSI-based network storage systems

Shiva Chaitanya, Kevin Butler, Anand Sivasubramaniam, Patrick McDaniel, Murali Vilayannur
October 2006 **Proceedings of the second ACM workshop on Storage security and survivability StorageSS '06**
Publisher: ACM Press
Full text available: pdf(296.66 KB) Additional Information: full citation, abstract, references, index terms

This paper studies the performance and security aspects of the iSCSI protocol in a network storage based system. Ethernet speeds have been improving rapidly and network throughput is no longer considered a bottleneck when compared to Fibre-channel based storage area networks. However, when security of the data traffic is taken into consideration, existing protocols like IPSec prove to be a major hindrance to the overall throughput. In this paper, we evaluate the performance of iSCSI when deploye ...

Keywords: IPSec, authentication, encryption, iSCSI

15 Data protection: Attribute-based encryption for fine-grained access control of encrypted data

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(277.46 KB) Additional Information: full citation, abstract, references, index terms

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and pri ...

Keywords: access control, attribute-based encryption, audit logs, broadcast encryption, delegation, hierarchical identity-based encryption

16 On the encipherment of search trees and random access files

R. Bayer, J. K. Metzger
March 1976 **ACM Transactions on Database Systems (TODS)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: pdf(1.30 MB) Additional Information: full citation, abstract, references, citings, index terms

The securing of information in indexed, random access files by means of privacy transformations must be considered as a problem distinct from that for sequential files. Not only must processing overhead due to encrypting be considered, but also threats to encipherment arising from updating and the file structure itself must be countered. A general encipherment scheme is proposed for files maintained in a paged structure in secondary storage. This is applied to the encipherment of indexes or ...

Keywords: B-trees, cryptography, encipherment, indexed sequential files, indexes, paging, privacy, privacy transformation, protection, random access files, search trees, security

17 A cryptographic file system for UNIX

Matt Blaze

December 1993. **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**

Publisher: ACM Press

Full text available: pdf(955.62 KB) Additional Information: full citation, abstract, references, citings, index terms

Although cryptographic techniques are playing an increasingly important role in modern computing system security, user-level tools for encrypting file data are cumbersome and suffer from a number of inherent vulnerabilities. The Cryptographic File System (CFS) pushes encryption services into the file system itself. CFS supports secure storage at the system level through a standard Unix file system interface to encrypted files. Users associate a cryptographic key with the directories ...

18 Practice: Some security alternatives for encrypting information on storage devices

Robin Snyder

September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**

Publisher: ACM Press

Full text available: pdf(63.12 KB) Additional Information: full citation, abstract, references, index terms

Almost every few weeks there is some breaking news about some organization that has lost information via the physical loss of an unencrypted storage device. This paper reviews some alternatives for encrypting information on storage devices and how those alternatives might be used. The open source TrueCrypt system is covered is some detail. Some suggestions for information security policy guidelines are provided. From personal data to enterprise data, information security is becoming increasin ...

Keywords: encrypting file systems, storage devices

19 Protecting file systems with transient authentication

Mark D. Corner, Brian D. Noble

January 2005 **Wireless Networks**, Volume 11 Issue 1-2

Publisher: Kluwer Academic Publishers

Full text available: pdf(422.63 KB) Additional Information: full citation, abstract, references, index terms

Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryptographic file system does not fully address this problem. Such systems ask the user to imbue them with long-term authority for decryption, but that authority can be used by anyone who physically possesses the

machine. Forcing the user to frequently reestablish his identity is intrusive, encouraging him to disable encryption.This tension between usability and secur ...

20 Cryptographic key management

Dahl A. Gerberick
May 1990 **ACM SIGSAC Review**, Volume 8 Issue 2
Publisher: ACM Press
Full text available: pdf(962.96 KB) Additional Information: full citation, abstract, index terms

There are two main issues concerning data security on networks; controlling access and the vulnerability of data communication links. A brief introduction to the various techniques which may be applied to these concerns are given in this paper.

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next